UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/596,003	02/08/2007	Maria Pilar Gonzalez Lopez	P18126-US1	1612

27045   7590   06/25/2010
ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER
KATSIKIS, KOSTAS J

ART UNIT	PAPER NUMBER
2441	

NOTIFICATION DATE	DELIVERY MODE
06/25/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

kara.coffman@ericsson.com
jennifer.hardin@ericsson.com
melissa.rhea@ericsson.com

	Application No.	Applicant(s)
Office Action Summary	10/596,003	GONZALEZ LOPEZ ET AL.
	Examiner	Art Unit
	Kostas Katsikis	2441

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _03 March 2010_.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _37-72_ is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) _37-72_ is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☐ All   b) ☐ Some * c) ☐ None of:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____.
      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)
1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March

3, 2010 has been entered.

2.   This communication is in response to RCE filed March 3, 2010, in which claims

37, 39-40, 44-45, 50-51, 55-56, 61-62, 66-67, and 72 have been amended.

Accordingly, claims 37-72 remain pending for examination.

Status of Claims

3.   Claims 37-72 are pending, of which claims 37-72 are rejected under 35 U.S.C.

103. Claims 37-50, and 62-72 are also rejected under 35 U.S.C. 101.

Claim Rejections - 35 USC § 101

4.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine,
> manufacture, or composition of matter, or any new and useful improvement

thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5.   **Claims 37-50 are rejected under 35 U.S.C. 101 because the claimed invention is directed to nonstatutory subject matter.**

As to claim 37, the "*Apparatus*" claim is not to a process, machine, manufacture or composition of matter. The claimed elements/limitations ["*communication receiver component*", "*management verifier component*", and "*communication sender component*" are non-structural limitations. Given the broadest reasonable interpretation in light of the supporting disclosure as mandated (MPEP §2106), the claimed elements/limitations are non-structural, and may be potentially interpreted as software. It is well known in the art that such mechanisms as those claimed (communication receiver component, management verifier component, and communication sender component) may be implemented in software, and the instant Specification fails to give any concrete evidence that these mechanisms are in fact hardware implemented. In addition, paragraphs [0033]-[0034] of the instant Specification recite, "*[0033] A simplified schematic functional view of some **functional components (201, 202, 203)** of an apparatus for mediating in management orders 200 according to the invention is given in Fig.2. **Said functional components can be accomplished according to various implementation alternatives that can comprise software, hardware or combinations of both.***

*[0034] The apparatus 200 comprises a **Communication Receiver Component CRC***

201 *as a functional component arranged to receive management orders from a plurality*

of origin managers (I01, 102 .... 10x)", which, in conjunction with FIG. 2, denote the

claimed components may be implemented entirely in software. Additionally, paragraph

[0035] of the instant Specification, in conjunction with FIG. 2, recites, "*Once the*

information elements referenced in a received management order have been extracted

from the content of said order, said information is passed to a ***Management Verifier***

Component MVC 202". Finally, paragraph [0036] of the instant Specification, in

conjunction with FIG. 2, evidences that, "*Finally, an approved management order is sent*

towards the managed device(s) affected by it (301, 302, 30x) by the ***Communication***

Sender Component CSC 203, *which is the functional element in the management*

mediating apparatus 200 that performs the equivalent reversal functions as the CRC

201". Therefore, the claimed subject matter as a whole fails to fall within the definition

of a process, <u>machine</u>, manufacture or composition of matter, patentable eligible

category subject matter. (see Interim Examination Instructions for Evaluating Subject

Matter Eligibility under 35 U.S.C. §101 memo available online at

<u>http://www.uspto.gov/patents/law/comments/2009-08-25_interim_101_instructions.pdf</u> .

These instructions as indicated in the memo supersede previous guidance on subject

matter eligibility that conflicts with the Instructions, including MPEP 2106(IV), 2106.01

and 2106.02 ([*see e.g. definition of "machine" p. 1, 3 and 5]*).

Dependent claims 38-50 fail to cure the deficiencies of independent claim 32 and are similarly rejected.

6.   Claims 62-72 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The United States Patent and Trademark Office (USPTO) is obliged to give claims their broadest reasonable interpretation consistent with the specification during proceedings before the USPTO. *See In re Zletz*, 893 F.2d 319 (Fed. Cir. 1989) (during patent examination the pending claims must be interpreted as broadly as their terms reasonably allow). The broadest reasonable interpretation of a claim drawn to a computer readable medium (also called machine readable medium and other such variations) typically covers forms of **non-transitory tangible media** and **transitory propagating signals per se** in view of the ordinary and customary meaning of computer readable media, particularly when the specification is silent. *See* MPEP 2111.01. When the broadest reasonable interpretation of a claim covers a signal *per se*, the claim must be rejected under 35 U.S.C. § 101 as covering non-statutory subject matter. *See In re Nuijten*, 500 F.3d 1346, 1356-57 (Fed. Cir. 2007) (transitory embodiments are not directed to statutory subject matter) and *Interim Examination Instructions for Evaluating Subject Matter Eligibility Under 35 U.S.C. § 101*, Aug. 24, 2009; p. 2.

The USPTO recognizes that applicants may have claims directed to computer readable media that cover signals *per se*, which the USPTO must reject under 35 U.S.C. § 101 as covering both non-statutory subject matter and statutory subject matter. In an effort to assist the patent community in overcoming a rejection or potential rejection under 35 U.S.C. § 101 in this situation, the USPTO suggests the following approach. A claim drawn to such a computer readable medium that covers both **transitory** and **non-transitory** embodiments may be amended to narrow the claim to cover only statutory embodiments to avoid a rejection under 35 U.S.C. § 101 by adding the limitation "**non-transitory**" to the claim. *Cf. Animals - Patentability*, 1077 *Off. Gaz. Pat. Office* 24 (April 21, 1987) (suggesting that applicants add the limitation "non-human" to a claim covering a multi-cellular organism to avoid a rejection under 35 U.S.C. § 101). Such an amendment would typically not raise the issue of new matter, even when the specification is silent because the broadest reasonable interpretation relies on the ordinary and customary meaning that includes signals *per se*. The limited situations in which such an amendment could raise issues of new matter occur, for example, when the specification does not support a non-transitory embodiment because a signal *per se* is the only viable embodiment such that the amended claim is impermissibly broadened beyond the supporting disclosure. *See, e.g., Gentry Gallery, Inc. v. Berkline Corp.*, 134 F.3d 1473 (Fed. Cir. 1998).

As per claims 62-72, as disclosed in paragraph [0032] of the instant Specification, "*Accordingly, the computer-based mediator 200 comprises: a*

communication interface COM arranged to receive and issue management orders, ***a***

data storage MEM *arranged to store processing instructions as well as other data to*

perform its specific operation, a processor PROC arranged to execute said processing

instructions, and internal data buses 20 to communicate these elements", which, given

the broadest reasonable interpretation, may include a ***transitory-type medium***

rendering the computer-readable medium ***transitory***, and thus able to be interpreted as

a signal. Signal is non-statutory subject matter, and as such independent claim 13 is

non-statutory.

Dependent claims 63-72 fail to cure the deficiencies of independent claim 62 and

are similarly rejected.

7.   **Examiner's Note:** Examiner has cited particular paragraphs and/or columns and

line numbers in the references applied to the claims below for the convenience of the

applicant. Although the specified citations are representative of the teachings of the art

and are applied to specific limitations within the individual claim, other passages and

figures may apply as well. It is respectfully requested from the applicant in preparing

responses, to fully consider the references in entirety as potentially teaching all or part

of the claimed invention, as well as the context of the passage as taught by the prior art

or disclosed by the Examiner.

Claim Rejections - 35 USC § 103

8.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed
> or described as set forth in section 102 of this title, if the differences between the
> subject matter sought to be patented and the prior art are such that the subject
> matter as a whole would have been obvious at the time the invention was made
> to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was
> made.

9.   **Claims 37-72 are rejected under 35 U.S.C. 103(a) as being unpatentable**

over Black et al. (United States Patent Application Publication No. US

2002/0116485 A1), hereinafter "Black" in view of Esko Freese (International Patent

Application Publication No. WO 02/19116 A2), hereinafter "Freese".

Regarding claims 37, 51, and 62, **Black** discloses an apparatus for mediating in

management orders between a plurality of origin managing devices and a plurality of

managed devices in a telecommunications system, the management orders intended to

execute management operations over the managed devices, comprising:

a communication receiver component arranged to receive a management order

from one of the origin managing devices *(wherein network management system (NMS)*

servers utilize templates to non-interactively connect Operation Support Services (OSS)

clients (origin managing devices) to managed devices (network devices), management

configuration tasks are originated in OSS clients and relayed to and received in NMS

servers, NMS server receives calls from OSS client to configure network devices)

(Black, FIG. 3b and 3h-3i combined, paragraphs [0112]-[0113], [0408]-[0416]);

a management access template, the management access template being one

selected from the group consisting of: a first management access template in

relationship with an identifier of the origin manager *(wherein three general categories of*

templates are utilized for provisioning management of network devices, first category,

control templates, connect OSS clients (origin managing devices) to NMS servers

(mediating apparatuses)) **(Black, FIG. 3h, paragraphs [0410]-[0411])**; a second

management access template in relationship with an identifier of a managed data object

affected by the management order *(wherein second category, provisioning template are*

used to issue appropriate calls to NMS server to modify data objects within

configuration database) **(Black, FIG. 3h, paragraphs [0410]-[0411])**; and a third

management access template in relationship with an identifier of a managed device

affected by the management order *(wherein third category is batch template associated*

with provisioning network devices) **(Black, FIG. 3h, paragraphs [0410]-[0411])**; and

a communication sender component arranged to send an allowed management

order to a managed device *(wherein NMS server relays template with instructions to*

configure corresponding network device) **(Black, FIG. 3b and 3h-3i combined,**

paragraphs [0112]-[0113], and [0408]-[0416]).

Black does not explicitly disclose a management verifier component arranged to

determine whether the received management order is an allowed management order by checking whether the management order fits an access attribute.

However **Freese** discloses a management verifier component arranged to determine whether the received management order is an allowed management order by checking whether the management order fits an access attribute *(wherein operator initiates sending of instruction from originating management console, containing identity of application to be controlled, and is cryptographically signed for authentication)* **(Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9)**.

Black and **Freese** are analogous art because they are from the same problem solving area, namely, management of client devices in telecommunications networks.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Black** and **Freese** before him or her, to modify the telecommunications management apparatus of **Black**, to include the cryptographic-authenticating-instruction functionality of **Freese**, with reasonable expectation that this would result in a system that guaranteed the security and reliability of received management instructions, without the requirement of special secure network management protocols such as SNMP Version 3, thereby allowing any compatible network management protocol to be used and not a specially enhanced version having built-in encryption and security. This approach to improving the telecommunications management apparatus of **Black** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Freese**.

Therefore, it would have been obvious to one of ordinary skill in the art to

combine the teachings of **Black** and **Freese** to obtain the invention as specified in claim 37.

Claim 62 includes a computer program for performing the limitations substantially as described in claim 37. **Black-Freese** discloses a computer program for mediating from a computer-based apparatus in management orders between a plurality of origin managers and a plurality of managed devices in a telecommunications system for performing the limitations substantially as described in claim 37 *(wherein computer system in telecommunications network with plurality of origin managers and plurality of managed devices includes centralized processor with control processor subsystem that executes instance of the kernel including master control and server programs to actively control system operation by performing major portion of control functions)* **(Black, FIG. 1, and FIG. 2a-2b, paragraphs [0103]-[0110], [0112]-[0118], and [0125]-[0126])**. The motivation regarding the obviousness of claim 37 is also applied to claim 62; therefore, claim 62 is rejected under the same rationale.

Additionally, claim 51 recites a method for mediating in the management of a plurality of devices from a plurality of origin managers that performs the limitations substantially as described in claims 37 and 62 and is rejected for similar reasons.

Regarding claim 38, **Black-Freese** discloses the apparatus of claim 37, wherein the first management access template further comprises at least one access attribute selected from the group consisting of: an identifier of an allowed management operation *(wherein instruction is identified with cryptographic signature)* **(Freese, FIG. 1-FIG. 2,**

page 5, line 23-page 6, line 9); an identifier of an allowed managed data object; a

pattern structure of the managed data object; an identifier of an allowed managed

device; an identifier of an allowed management operation over an allowed managed

device; and an identifier of an allowed management operation over an allowed

managed data object. The motivation regarding the obviousness of claim 37 is also

applied to claim 38.

Regarding claim 39, **Black-Freese** discloses the apparatus of claim 37, wherein

the second management access template further comprises at least one access

attribute selected from the group consisting of: a pattern structure of the managed data

object; an identifier of an allowed management operation *(wherein instruction is*

identified with cryptographic signature) **(Freese, FIG. 1-FIG. 2, page 5, line 23-page 6,**

line 9); an identifier of a managed device holding the managed data object; an identifier

of an allowed origin managing device; an identifier of an allowed management operation

from an allowed origin managing device; and an identifier of an allowed management

operation over a holding managed device. The motivation regarding the obviousness of

claim 37 is also applied to claim 39.

Regarding claim 40, **Black-Freese** discloses the apparatus of claim 37, wherein

the third management access template comprises at least one access attribute selected

from the group consisting of: an identifier of an allowed management operation *(wherein*

instruction is identified with cryptographic signature) **(Freese, FIG. 1-FIG. 2, page 5,**

line 23-page 6, line 9); an identifier of a managed data object held on the managed

device; an identifier of an allowed origin managing device; an identifier of an allowed

management operation from an allowed origin managing device; and an identifier of an

allowed management operation over a held managed data object. The motivation

regarding the obviousness of claim 37 is also applied to claim 40.

Regarding claim 41, **Black-Freese** discloses the apparatus of claim 37, wherein

the management verifier component is arranged to determine, from the identifier of a

management operation, at least one identifier, the identifier being one selected from the

group consisting of: an identifier of a managed data object affected by the operation;

and an identifier of a managed device, affected by the operation *(wherein the header of*

the SMS message contains the phone number identifying the device affected by the

operation) **(Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9)**. The motivation

regarding the obviousness of claim 37 is also applied to claim 41.

Regarding claim 42, **Black-Freese** discloses the apparatus of claim 37, wherein

the management verifier component is arranged to select a management access

template, among the first second and third management templates, according to an

identifier received in a management order *(wherein a number of various management*

templates may be transmitted to NMS server from OSS client, templates with

instructions may be selected after verified via verification component) **(Black, FIG. 3b**

and 3h-3i combined, paragraphs [0408]-[0416], Freese, FIG. 1-FIG. 2, page 5, line

23-page 6, line 9). The motivation regarding the obviousness of claim 37 is also

applied to claim 42.

Regarding claim 43, **Black-Freese** discloses the apparatus of claim 42, wherein

the management verifier component is arranged to select a management access

template, among the first second and third management templates, according to an

access attribute comprised in another selected management access template *(wherein*

template may be selected and verified based on identification of authorized

cryptographic signature, which is comprised in other templates) **(Black, FIG. 3b and**

3h-3i combined, paragraphs [0408]-[0416], Freese, FIG. 1-FIG. 2, page 5, line 23-

page 6, line 9). The motivation regarding the obviousness of claim 37 is also applied to

claim 43.

Regarding claim 44, **Black-Freese** discloses the apparatus of claim 42, wherein

the identifier of the origin managing device comprises at least one identifier selected

from the group consisting of: an identifier of a management server sending a

management order; and an identifier of a user operating the management server

(wherein network manager may need to supply username and password upon

establishing connection with OSS client, NMS server, and corresponding network

device) **(Black, FIG. 3i, paragraphs [0415]-[0416])**; and

wherein the management verifier component is arranged to select the first

management access template according to the at least one identifier *(wherein verifier*

selects management instructions upon verifying cryptographic signature) **(Freese, FIG.**

1-FIG. 2, page 5, line 23-page 6, line 9). The motivation regarding the obviousness of

claim 37 is also applied to claim 44.

Regarding claim 45, **Black-Freese** discloses the apparatus of claim 42, wherein

the identifier of the origin managing device comprises at least one identifier selected

from the group consisting of: an identifier of a management server sending a

management order; and an identifier of a user operating the management server

(wherein network manager may need to supply username and password upon

establishing connection with OSS client, NMS server, and corresponding network

device) **(Black, FIG. 3i, paragraphs [0415]-[0416])**; and wherein the management

verifier component is arranged to authenticate the at least one identifier *(wherein verifier*

selects management instructions upon verifying cryptographic signature) **(Freese, FIG.**

1-FIG. 2, page 5, line 23-page 6, line 9). The motivation regarding the obviousness of

claim 37 is also applied to claim 45.

Regarding claim 46, **Black-Freese** discloses the apparatus of claim 42, wherein

the management verifier component is arranged to determine a management role

associated to at least one identifier, the identifier being one selected from the group

consisting of: an identifier of a management server sending a management order; and

an identifier of a user operating the management server *(wherein network manager may*

need to supply username and password upon establishing connection with OSS client,

NMS server, and corresponding network device) **(Black, FIG. 3i, paragraphs [0415]-**

[0416]). The motivation regarding the obviousness of claim 37 is also applied to claim

46.

        Regarding claim 47, **Black-Freese** discloses the apparatus of claim 46, wherein

the management verifier component is further arranged to select at least one

management access template in relationship with the role *(wherein network manager*

may need to supply username and password upon establishing connection with OSS

client, NMS server, and corresponding network device, verifier selects management

instructions upon verifying cryptographic signature) **(Black, FIG. 3i, paragraphs [0415]-**

[0416], Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9). The motivation

regarding the obviousness of claim 37 is also applied to claim 47.

        Regarding claim 48, **Black-Freese** discloses the apparatus of claim 46, wherein

at least one management access template among the second or third management

templates comprises an identifier (ROm) of at least one role as an access attribute, and

wherein the Management Verifier Component is further arranged to check whether the

management order fits with the role *(wherein batch templates may contain names of*

control templates to cause OSS client to issue calls to NMS server affecting

corresponding network device, authorized network manager non-interactively

completing provisioning tasks and building custom services) **(Black, FIG. 3b,**

paragraphs [0410]-[0411]). The motivation regarding the obviousness of claim 37 is

also applied to claim 48.

Regarding claim 49, **Black-Freese** discloses the apparatus of claim 37, wherein

the management verifier component is arranged to determine whether a managed data

object affected by an allowed management order is an access attribute in a

management access template, and further comprising a management execution

component, arranged to execute a management operation over the access attribute

(wherein templates comprise various parameter values which affect data objects, may

be provisioned by network managers upon establishing connections with NMS server

and network devices, while verifier component verifies and determines whether object is

known attribute, (i.e., antivirus signatures previously identified and stored in database,

used to identify viruses in scanned data), upon authentication, management agent may

update signature database and execute instruction) **(Freese, FIG. 1-2, page 6, lines**

17-26). The motivation regarding the obviousness of claim 37 is also applied to claim

49.

Regarding claim 50, **Black-Freese** discloses the apparatus of claim 37, wherein

the communication receiver component is further arranged to receive an access request

from one of the origin managing devices *(wherein NMS server issues provisioning*

requests for template in response to calls from OSS client) **(Black, FIG. 3h, paragraph**

[0414]);

wherein the management verifier component is further arranged to determine the

first management access template *(wherein verifier component determines whether instruction is authorized)* **(Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9)**; and

wherein the communication sender component is further arranged to send an access response to the origin managing device that comprises an access attribute of the management access template *(wherein network manger may send command to interactive interpreter to cause OSS client to display available and acceptable parameter values for each template)* **(Black, FIG. 3i, paragraphs [0417]-[0418])**. The motivation regarding the obviousness of claim 37 is also applied to claim 50.

Claims 52-61 are corresponding method claims of apparatus claims 41-50; therefore, they rejected under the same rationale.

Claims 63-72 are corresponding computer program claims of apparatus claims 41-50; therefore, they are rejected under the same rationale.

Response to Arguments

10.   Applicant's arguments, see pages 12-17, filed March 3, 2010, with respect to Rejections of Claims 37-72 under 35 U.S.C. § 103(a) have been fully considered but they are not persuasive.

11.   In the Remarks, Applicant argued in substance that

(A)   Applicant argued on pages 13-14 of the Remarks, the claimed apparatus's configuration where it mediates an management order from an origin managing device (not a person such as network managers/administrators) to determine if it is an allowed management order and if yes then sends the allowed management order to a managed device is not taught or suggested by **Black**, **Freese** or any combination thereof **(Recited from page 13 of Remarks)**. **Black's** OSS does not interface with <u>origin managing devices</u> nor does the OSS receive a management order from one of the <u>origin managing devices</u> to determine if it is an allowed management order and if yes then sends the allowed management order to a managed device. The Examiner can appreciate that **Black's** network managers/administrators are not the claimed origin managing devices. Thus, **Black** does not anticipate the presently claimed invention **(Recited from page 14 of Remarks)**.

As to point **(A),** Examiner respectfully disagrees, in that **Black** does disclose the newly claimed limitations of

a communication receiver component arranged to receive a management order from one of the origin managing devices

a management access template, the management access template being one selected from the group consisting of:

a first management access template in relationship with an identifier of the origin manager

a second management access template in relationship with an identifier of a

managed data object affected by the management order; and

a third management access template in relationship with an identifier of a

managed device affected by the management order; and

a communication sender component arranged to send an allowed management

order to a managed device.

Specifically, **Black** discloses a network management system (NMS), comprised

of NMS servers and NMS clients, to alleviate the need for network administrators to

directly access and configure the network devices **(See Black, paragraphs [0108]-**

[0113], and [0123]). In particular, **Black** discloses NMS servers that utilize templates to

non-interactively connect Operation Support Services (OSS) clients (origin managing

devices) to managed devices (network devices) **(See Black, paragraphs [0409]-**

[0408]). **Black** clearly states that services may be provisioned on one or more network

devices, ***instead of using a GUI***, ***non-interactively***, with the use of templates and the

operations support services client OSS **(See Black, paragraph [0408])**. **Black**

discloses management configuration tasks are originated in OSS clients and relayed to

and received in NMS servers, which receive calls from an OSS client to configure the

corresponding network devices **(See Black, FIG. 3b and 3h-3i combined, paragraphs**

[0112]-[0113], [0408]-[0416]). **Black** further discloses three general categories of

templates are utilized for provisioning management of network devices. The first

category, termed control templates, connect OSS clients (origin managing devices) to

NMS servers (mediating apparatuses). Instead of connecting the OSS client with a

particular NMS server and then causing the NMS server to connect to a particular

device, **Black** discloses that a control template may be used to ***non-interactively***

establish the connections **(See Black, FIG. 3h, paragraph [0410])**. The second

category, termed provisioning templates, are used to issue appropriate calls to NMS

server to modify data objects within the configuration database of the appropriate

network device **(See Black, FIG. 3h, paragraphs [0410]-[0411])**. Additionally, **Black**

discloses the third category, termed batch templates, are associated with provisioning

larger amounts of services and network devices directly within one concatenated

template **(See Black, FIG. 3h, paragraphs [0410]-[0411])**. **Black** later discloses the

NMS server relays the template with instructions to configure corresponding network

device **(See Black, FIG. 3b and 3h-3i combined, paragraphs [0112]-[0113], and**

[0408]-[0416]).

Thus, Examiner respectfully submits that **Black** does anticipate the presently

claimed invention with the amended claim limitations. Due to the amendment, however,

Examiner has updated citations of each limitation to more accurately reflect claim

mappings.

(B)   Applicant argued on page 16 of the Remarks, **Black** does not disclose a

"template" in relationship with an identifier of the origin manager, so as to determine

whether a received management order is an allowed management order, before

sending it to a managed device **(Recited from page 16 of Remarks)**.

As to point **(B),** Examiner respectfully disagrees, noting that, as mentioned

above, **Black** discloses three categories of templates, Batch, control, and provisioning

templates. Control templates non-interactively establish connections among NMS

servers and OSS clients, while provisioning templates may be used to complete

particular provisioning tasks. Batch templates may also be used to concatenate a

series of templates to provision many network devices, and non-interactively

provisioning larger amounts of services. **Black** discloses that Database view ids and

APIs for the OSS client (origin managing device) may be generated using the logical

model and code generation system (FIG. 3b) to synchronize the integration interfaces

between the OSS clients and the NMS servers (mediating apparatuses) **(See Black,**

FIG. 3b, paragraphs [0410]-[0411]).

Thus, Examiner respectfully submits that **Black** does disclose a "template" in

relationship with an identifier of the origin manager. As mentioned above at items 8-9,

Black does not explicitly disclose determining whether a received management order is

an allowed management order, before sending it to a managed device.

However **Freese** discloses a management verifier component arranged to

determine whether the received management order is an allowed management order by

checking whether the management order fits an access attribute *(wherein operator*

initiates sending of instruction from originating management console, containing identity

of application to be controlled, and is cryptographically signed for authentication)

(Freese, FIG. 1-FIG. 2, page 5, line 23-page 6, line 9).

Black and **Freese** are analogous art because they are from the same problem

solving area, namely, management of client devices in telecommunications networks.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of **Black** and **Freese** before him or her, to modify the telecommunications management apparatus of **Black**, to include the cryptographic-authenticating-instruction functionality of **Freese**, with reasonable expectation that this would result in a system that guaranteed the security and reliability of received management instructions, without the requirement of special secure network management protocols such as SNMP Version 3, thereby allowing any compatible network management protocol to be used and not a specially enhanced version having built-in encryption and security. This approach to improving the telecommunications management apparatus of **Black** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Freese**.

Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of **Black** and **Freese** to obtain the invention as specified in the claim.

Thus, Examiner respectfully submits that **Black-Freese** does disclose the claimed limitations.

(C)   Applicant argued on page 16 of the Remarks, Examiner stated the following "**Black** does not explicitly disclose a management verifier component arranged to determine whether the received management order is an allowed management order by checking whether the management order fits an access attribute" (see page 4 in

Office Action). Applicant submits that the Examiner has also failed to mention or

address where the claimed "access attribute" is comprised in a management access

"template" held by the management verifier component **(Recited from page 16 of**

Remarks).

As to point **(C),** Examiner respectfully notes that in response to applicant's

arguments against the references individually, one cannot show nonobviousness by

attacking references individually where the rejections are based on combinations of

references. See *In re Keller,* 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck &*

Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

In this instant case, Applicant is attacking each reference individually, stating the

missing "access attribute", which is *not taught* by **Black**, but rather disclosed in

Freese, is not adequately disclosed in **Freese**, since the claimed "access attribute" is

not comprised in a management access "template" held by the management verifier

component.

The management access "template", however, is disclosed in **Black**, wherein

Black discloses three categories of templates, Batch, control, and provisioning

templates. Control templates non-interactively establish connections among NMS

servers and OSS clients, while provisioning templates may be used to complete

particular provisioning tasks. Batch templates may also be used to concatenate a

series of templates to provision many network devices, and non-interactively

provisioning larger amounts of services. Examiner respectfully submits that it is the

combination of **Black** with **Freese**, such that to modify the telecommunications

management apparatus of **Black**, to include the cryptographic-authenticating-instruction

functionality of **Freese** such that the identity of the application to be controlled were

superimposed within a provisioning template such as that of **Black**, to be

cryptographically signed for authentication, with reasonable expectation that this would

result in a system that guaranteed the security and reliability of received management

instructions, without the requirement of special secure network management protocols

such as SNMP Version 3, thereby allowing any compatible network management

protocol to be used and not a specially enhanced version having built-in encryption and

security. This approach to improving the telecommunications management apparatus

of **Black** was well within the ordinary ability of one of ordinary skill in the art based on

the teachings of **Freese**.

Moreover, the limitation of *management access "template"* ***held by the***

management verifier component is not positively recited in the claim language and

therefore not being given patentable weight. There is absolutely no mention anywhere

in the claim of the ***management access "template"*** being ***held by the management***

verifier component. As can be seen from the instant claim language, the above

referenced limitation of claim 37 recites

> ***a management verifier component arranged to determine whether the***
>
> ***received management order is an allowed management order by checking***
>
> ***whether the management order fits an access attribute comprised in a***
>
> ***management access template, the management access template being one***

selected from the group consisting of:

Examiner respectfully submits that if the limitation of *management access*

"template" **held by the management verifier component** is in fact a critical feature of

the invention, then it should be present in the claim language.

Thus, Examiner respectfully submits that **Black-Freese** does disclose the

claimed limitations.

(D)   Applicant argued on pages 16-17 of the Remarks, Applicant submits that

Freese (or **Black**) does not disclose a management verifier component within an entity,

mediating provisioning orders between a plurality of origin managers, and a plurality of

managed devices **(Recited from pages 16-17 of Remarks)**.

As to point **(D),** Examiner respectfully disagrees. As noted above, **Freese**

discloses a management verifier component arranged to determine whether the

received management order is an allowed management order by checking whether the

management order fits an access attribute. An operator initiates sending of instruction

from originating management console, containing the ID of the application to be

controlled, and is cryptographically signed for authentication **(See Freese, FIG. 1-FIG.**

2, page 5, line 23-page 6, line 9).

Additionally, as noted above, Examiner respectfully submits that the combination

of **Black** with **Freese**, such that to modify the telecommunications management

apparatus of **Black**, to include the cryptographic-authenticating-instruction functionality

of **Freese** such that the identity of the application to be controlled were superimposed within a provisioning template such as that of **Black**, to be cryptographically signed for authentication, with reasonable expectation that this would result in a system that guaranteed the security and reliability of received management instructions, without the requirement of special secure network management protocols such as SNMP Version 3, thereby allowing any compatible network management protocol to be used and not a specially enhanced version having built-in encryption and security. This approach to improving the telecommunications management apparatus of **Black** was well within the ordinary ability of one of ordinary skill in the art based on the teachings of **Freese**. Examiner has already shown at least in **(A)** of Response to Arguments Section, that **Black** discloses mediating provisioning orders between a plurality of origin managers, and a plurality of managed devices.

Thus together, **Black-Freese** disclose all of the amended claimed limitations.

Conclusion

12. Applicant's arguments as well as request for reconsideration filed on March 3, 2010 have been fully considered but they are not deemed to be persuasive.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kostas Katsikis whose telephone number is (571)270-5434. The examiner can normally be reached on Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Wing Chan can be reached on (571)272-7493. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Wing F. Chan/   /Kostas Katsikis/
Supervisory Patent Examiner, Art Unit 2441   Examiner
                                                                Art Unit 2441

June 17, 2010